Remarks/Arguments

The Office Action mailed February 2, 2009 has been reviewed and carefully considered. No new matter has been added. Claim 27 has been amended. Claims 1, 6-9, 16, and 18-35 are pending in this application. Reconsideration of the above-identified application, in view of the above amendments and the following remarks, is respectfully requested.

Claims 25, 29, and 33 stand rejected under 35 U.S.C. 112, second paragraph. The rejection is respectfully traversed.

With respect to Claim 25, it is believed that said claim is proper as written, is supported by the specification, and is NOT in contradiction with respect to the operation of the subject matter of Claim 23. For example, in Claim 23, the respective one of the plurality of user discernable indicators (hereinafter respective indicator) is triggered when one or more rules corresponding to one of said plurality of classes associated with the respective indicator is violated (as primarily set forth in Claim 1, from which Claim 23 depends). However, according to Claim 23, the particular one of the plurality of user discernable indicators (hereinafter particular indicator), which is associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules, is only triggered when a number of the packets that violate the one or more rules exceeds a pre-specified threshold. In Claim 25, even though the one or more rules are violated resulting in filtering being performed by the firewall program, only the respective indicator is triggered (i.e., NOT along with the particular indicator) when the number of the packets that violate the one or more rules does NOT exceed the pre-specified

threshold. Hence, Claim 25 is essentially the compliment to Claim 23. Thus, in Claim 23 the particular indicator is triggered, along with the respective indicator, when a number of the packets that violate the one or more rules exceeds a pre-specified threshold, while in Claim 25 the particular indicator is NOT triggered when the number of the packets that violate the one or more rules does NOT exceed the pre-specified threshold. Hence, even through the particular indicator is associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules, the particular indicator is still nonetheless triggered (and thus apparent to the user) only when the number of packets that violate the one or more rules exceeds a pre-specified threshold. The Examiner's statement that the particular indicator would be contemporaneously going off as soon as the first packet broke a rule regardless of the threshold is incorrect. The fact that the particular indicator is associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules does not by itself govern whether the particular indicator is triggered (and is, thus, apparent to the user). Rather, the threshold governs the triggering of the particular indicator. For example, being associated is not the same as being triggered. This is explicitly supported by page 12, lines 20-24 of the Applicants' specification, which discloses the following:

> [T]he firewall program 124 may filter out all data packets violating a particular firewall program rule, but will only trigger the indicator if the threshold level has been exceeded. For example, all packets found violating the third class rules in step 314 are immediately filtered, however, the

indicator 126 will only be triggered once the threshold level of illustrative step 316 has been exceeded.

The preceding is not contrary to the purpose of the invention, as the user is provided with the respective indicator when a rule violation has occurred. However, an inherent degree of violation, as represented by an amount of violating packets above a given threshold, may also be concurrently provided by the particular indicator (along with the respective indicator).

Claims 29 and 33 are based on the same underlying reasoning with respect to the respective indicator and the particular indicator and, hence, the above arguments are reasserted with respect to Claims 29 and 33.

In view of the preceding, it is believed that Claims 25, 29, and 33 satisfy 35 U.S.C. 112, second paragraph. Reconsideration of the rejection is respectfully requested.

Claims 27, 28, and 29 stand rejected under 35 U.S.C. 112, second paragraph. Claim 27, from which Claims 28 and 29 depend, has been amended to now recite, *inter alia*, "a first class from among the plurality of classes", thus correcting the lack of antecedent basis as well as defining the first class as being one of the plurality of classes. In view of the preceding, it is believed that Claims 27, 28, and 29 satisfy 35 U.S.C. 112, second paragraph. Reconsideration of the rejection is respectfully requested.

As best understood from the Office Action, Claims 1, 6, 7, 8, 9, 20, 21, 23, 27, 24, 28, 25, 29, 26, 30, and 35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over ZoneAlarm publication by Ash Nallawalla (hereinafter "ZoneAlarm") in view of U.S. Patent Publication No. 2002/0178383 to Hrabik et al. (hereinafter "Hrabik"). Moreover, as best understood from the Office Action, Claims 16, 19, 18, 19, 22, 31, 32, 33, and 34 stand rejected under as being unpatentable over ZoneAlarm in view of Hrabik and in view of U.S. Patent No. 6,185,624B1 to Fijolek et al. (hereinafter "Fijolek"). The rejection is respectfully traversed.

The independent Claims currently pending are Claims 1, 7, and 16.

Regarding Claims 1, 7, and 16, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in each of Claims 1, 7, and 16: "wherein the rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels".

The Examiner has cited paragraph [0060] of Hrabik as disclosing the same, reasoning "In an effort to only interrupt a system administer with the utmost critical alerts, Hrabik teaches a firewall system in which the threats are prioritized and put into classes whereby only the higher classes are immediately sent to a system engineer for responsive actions". The Applicants respectfully disagree with the Examiner's reading of Hrabik.

The only seemingly relevant part of paragraph [0060] of Hrabik with respect to the above limitations is as follows:

> The target network can be divided into a plurality of security zones. Different security zones might differ in their importance to the company and, thus, have a different level of security risk. Accordingly, each uploaded security event may be further classified by its level of security risk in accordance with the security zone where it was last detected.

Claims 1, 7, and 16 involve and explicitly recite, *inter alia*, rules, classes, and priority levels. In further detail, Claims 1, 7, and 17 essentially recite that the rules in a set of rules (included in a firewall) are separated into a plurality of classes and prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels. The cited portion of Hrabik makes no explicit mention of rules, or classes, or priority levels. All that is disclosed in paragraph [0060] of Hrabik is that each uploaded security event may be further classified by its level of security risk in accordance with the security zone where it was last detected. Hence, the actual event itself is being classified based on which security zone the event was last detected. Thus, contrary to the rules in the set being separated into a plurality of classes (and hence classified), Hrabik directly classifies the actual event itself. That is, in the case of Hrabik, the classification (and, hence, class) of the actual event is the security risk (priority level), without regard to any underlying rule. Prioritizing a rule as explicitly claimed in Claims 1, 7, and 16 does not correspond to prioritizing an actual event itself. For example, a rule

is what is compared against an actual event to determine whether the rule is violated by the event in the first place. Hence, there is, for lack of a better term, a layer missing in the approach of Hrabik, as essentially admitted by the Examiner. That is, while Claims 1, 7, and 16 recite, *inter alia*, separating rules in a set into a plurality of classes and prioritizing the rules such that each of the classes represents a respective different priority level, in contrast **as admitted by the Examiner** Hrabik discloses "the threats are prioritized and put into classes" (Office Action, dated February 2, 2009, p. 6). For example, even the Examiner noted the preceding distinction in the Office Action, as follows;

> **ZoneAlarm** is silent in explicitly disclosing ***the rules in the set are prioritized*** **such that each of the plurality of classes represents a respective different one of a plurality of priority levels**. In an effort to only interrupt a system administrator with the utmost critical alerts, *Hrabik* teaches a firewall system in which *the threats are prioritized and put into classes* whereby only the higher classes are immediately sent to a system engineer for responsive actions (0060). Hrabik classifies threads but [sic-based] the security risk to the network.

Hence, based on the preceding, neither ZoneAlarm nor Hrabik teach or suggest "wherein the rules in the set are prioritized such that each of the plurality of classes

represents a respective different one of a plurality of priority levels", as recited in Claims 1, 7, and 16.

Moreover, it is respectfully asserted that even assuming arguendo that all of the recited limitations are taught by the cited combination, the rejection must be withdrawn because the combination (of ZoneAlarm and Hrabik) is improper, as the combination would change the principle of operation of the primary reference ZoneAlarm which is prohibited under MPEP §2143.01. That is, the combining of ZoneAlarm and Hrabik would change the principle of operation of ZoneAlarm and, as such, renders the combination improper under MPEP §2143.01.

For example, as set forth in MPEP §2143.01:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (Claims were directed to an oil seal comprising a bore engaging portion with outwardly biased resilient spring fingers inserted in a resilient sealing member. The primary reference relied upon in a rejection based on a combination of references disclosed an oil seal wherein the bore engaging portion was reinforced by a cylindrical sheet metal casing. Patentee taught the device required rigidity for operation, whereas the claimed invention required resiliency. The court reversed the rejection

> holding the "suggested combination of references would require a substantial reconstruction and redesign of the elements shown in [the primary reference] as well as a change in the basic principle under which the [primary reference] construction was designed to operate." 270 F.2d at 813, 123 USPQ at 352.).

Hence, in the instant case, as alleged by the Examiner, ZoneAlarm is a rule and class based system (see, e.g., Office Action dated February 2, 2009, pp. 4-5), while Hrabik is not for all the reasons set forth above. Thus, any modification of ZoneAlarm with the teachings of Hrabik to obtain the subject matter claimed in Claims 1, 7, and 16 would effectively remove the rule and class basis of ZoneAlarm, as Hrabik directly classifies actual threats with a priority level as set forth in detail herein above, essentially removing a "layer" that is allegedly present in ZoneAlarm and changing its principle of operation. Hence, in view of the preceding, the combination of ZoneAlarm and Hrabik must be withdrawn under MPEP §2143.01.

Thus, it is respectfully asserted that the cited combination of ZoneAlarm and Hrabik does not teach or suggest the above recited limitations of Claims 1, 7, and 16. Moreover, the remaining references do not cure the deficiencies of ZoneAlarm and/or Hrabik, and are silent with respect to the above recited limitations of Claims 1, 7, and 16.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art" (MPEP §2143.03, citing *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)).

Moreover, as argued above, the cited combination of ZoneAlarm and Hrabik is improper under MPEP §2143.01, thus mandating the withdrawal of the corresponding rejection.

Thus, Claims 1, 7, and 16 are patentable distinct and non-obvious over the cited references for at least the reasons set forth above.

Moreover, "[i]f an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

Claims 6, 20, 23, 26, and 35 directly depends from Claim 1, and thus include all the limitations of Claim 1. Claims 8, 9, 21, 27, and 30 directly depend from Claim 7, and thus include all the limitations of Claim 7. Claims 18, 19, 22, 31, and 34 directly depend from Claim 16, and thus include all the limitations of Claim 16. Accordingly, Claims 6, 20, 23, 26, and 35 are patentably distinct and non-obvious over the cited reference for at least the reasons set forth above with respect to Claim 1, Claims 8, 9, 21, 27, and 30 are patentably distinct and non-obvious over the cited reference for at least the reasons set forth above with respect to Claim 7, and Claims 18, 19, 22, 31, and 34 are patentably distinct and non-obvious over the cited reference for at least the reasons set forth above with respect to Claim 16.

Moreover, said dependent claims include patentable subject matter in and of themselves and are, thus, patentable distinct and non-obvious over the cited references in their own right. The limitations of the dependent claims to be argued will first be set forth sequentially, followed by arguments in favor of said dependent claims, as

essentially the same portions of the references and same rationale were applied against most of the following claims.

For example, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 20:

> wherein the firewall filters any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules, but only triggers the respective one of the plurality of user discernable indicators when the number of the packets that violate the one or more rules exceeds a pre-specified threshold.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 21:

> wherein the data traffic includes a number of packets that violate the at least one of the rules of the first one of the plurality of classes, and
> wherein the method filters the packets that violate the at least one of the rules of the first one of the plurality of classes, irrespective of the number of packets that violate the one or more rules, but only triggers the respective one of the plurality of user discernable indicators when the

number of packets that violate the at least one of the rules of the first one of the plurality of classes exceeds a pre-specified threshold.

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 22:

wherein the firewall program is executable by said controller to cause filtering of any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules, but wherein the respective one of the plurality of user discernable indicators is triggered only when the number of packets that violate the one or more rules exceeds a pre-specified threshold.

Also, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 23:

wherein each of the plurality of user discernable indicators except a particular one is associated with the respective different one of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being

contemporaneously performed for any of the packets that violate the one or more rules, and wherein the method further comprises filtering any of the packets that violate the one or more rules, and wherein the particular one of the plurality of user discernable indicators is concurrently triggered, along with the respective one of the plurality of user discernable indicators, to indicate that the filtering is being contemporaneously performed, only when a number of the packets that violate the one or more rules exceeds a pre-specified threshold.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 24:

wherein only the particular one of the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed the pre-specified threshold.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 25:

wherein only the respective one of the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed the pre-specified threshold.

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 26: "wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation."

Also, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 27:

wherein each of the plurality of user discernable indicators except a particular one is associated with the different one of the plurality of classes, and the method further comprises:

associating the particular one of the plurality of user discernable indicators with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate at least one of the rules; and

in the case of the rule of at least the first class being violated and a number of packets violating the rule of at least the first class exceeding a pre-specified threshold, providing a user discernable notification of the filtering being contemporaneously performed by triggering, concurrently with the triggering of the respective one of the plurality of user discernable indicators, the particular one of the plurality of user discernable indicators associated with the affirmative status that the filtering is being contemporaneously performed.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 28:

wherein in the case of the rule of at least the first class being violated and the number of packets violating the rule of at least the first class not exceeding the pre-specified threshold, only providing the user discernable notification of the filtering without providing the user discernable notification of the violation.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 29:

wherein in the case of the rule of at least the first class being violated and the number of packets violating the rule of at least the first class not exceeding the pre-specified threshold, only providing the user discernable notification of the violation without providing the user discernable notification of the filtering.

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 30: "wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation."

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 31:

wherein the firewall program is executable by said controller to cause filtering any of the packets that at least one of the rules, and wherein each of the plurality of user discernable indicators other than a particular one is respectively associated with the different ones of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being

contemporaneously performed, and wherein the particular one of the plurality of user discernable indicators is triggered, concurrently with the triggering of the respective one of the plurality of user discernable indicators, if the one or more of the rules is violated, the filtering is performed by the firewall program, and a number of the packets that violate the one or more rules exceeds a pre-specified threshold.

Also, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 32:

wherein only the particular one of the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed a pre-specified threshold.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 33:

wherein only the respective one of the plurality of user discernable indicators is triggered if the one or more of the rules is violated, the filtering is performed by the firewall program, and the number of the packets that violate the one or more rules does not exceed a pre-specified threshold.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 34: "wherein whether the respective one of the plurality of user discernable indicators is triggered or not is based on which of the plurality of priority levels is involved with respect to a corresponding rule violation."

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations recited in new Claim 35: "where each of the plurality of classes uses a different one of a plurality of thresholds with respect to how many violating ones of the packets must be detected before filtering is commenced, the plurality of thresholds being end-user settable."

With respect to the preceding, the Examiner has stated that "ZoneAlarm is silent in disclosing determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator. Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator (0059, 0060)." The Applicants respectfully disagree. Paragraph 0059 of Hrabik simply discloses: "A network event analyzer analyzes data in various views,

described above, looking for events exceeding predetermined thresholds." Paragraph 0060 of Hrabik simply discloses: "The master system 60 may also utilize risk threshold criteria against which all uploaded security events are compared. When an uploaded event exceeds a risk threshold, automatic countermeasures may be implemented." However, none of the preceding cited portions of Hrabik even remotely disclose premising whether a user discernable indication is provided based on a threshold as recited. Moreover, with respect to Claims 26 and 30, while the Examiner has simply stated that "Hrabik teaches the priority levels of the threat determine the countermeasure (0060)". However, paragraph [0060] of Hrabik is completely silent with respect to user discernable indicators, and a countermeasure is a measure taken to fix the threat and not necessarily to alert a user to the same.

It is to be noted that for some claims such as, e.g., Claims 23 and 27, the Examiner has stated the following on page 11 of the Office Action dated February 2, 2009:

> To reduce the number of false alarms, thresholds are a means to monitor events for suspicious activities. A single occurrence of a packet may not be anything harmful. However, if the occurrences start to add up quickly, that is a sign of a problem. Being able to determine a threshold also allows the system to detect benign traffic which is being used for malicious purposes. Having this ability strengthens the system. Therefore it would have been obvious to one of ordinary skill in the art at the time of the

invention to combine the use of threshold determination in a firewall to both not block normal traffic but to also block normal traffic being used maliciously.

However, the Examiner's reasoning has nothing to do with the actual claim limitations. What some of the preceding claims are reciting, *inter alia*, is that a user ascertainable indicator (as provided by one of the particular indicator or the respective indicator) is triggered (to alert a user) depending upon a threshold. The claims do not recite, as alleged by the Examiner on, for example, page 11 of the Office Action dated February 2, 2009 with respect to Claims 23 and 27, that the threshold serves to strengthen or weaken any blocking activity that may be performed by the firewall program. Hence, in view of the Examiner's incorrect interpretation of the claims, it is respectfully and earnestly requested that the Examiner re-evaluate the pending claims against the cited references.

With respect to Claim 35, said claim explicitly recites, *inter alia*, that the plurality of thresholds are end-used settable. In contrast, on page 12 of the Office Action dated February 2, 2009, the Examiner has stated that "[i]t is inherent from reading the teaching of Hrabik that the system engineer must be responsible for setting the threshold levels. However, the "security" engineer disclosed in Hrabik is not an end-user. For example, as disclosed at paragraph [0060] of Hrabik, "When an event is uploaded for review by the master system 60, a single ticket is generated for all security events determined to be related to the same attack, and a security engineer immediately begins researching the

information in the ticket." Thus, the security engineer is not an end-user but rather the person tasked with solving the problem encountered by the end-user.

Thus, with respect to the limitations recited in Claims 20-35, it is respectfully asserted that the cited references, taken singly or in any combination, do not teach or suggest the same, and appear to be silent with respect to the above limitations of Claims 20-35.

Thus, reconsideration of the above rejections is respectfully requested.

In view of the foregoing, Applicants respectfully request that the rejection of the claims set forth in the Office Action of February 2, 2009 be withdrawn and that the pending claims be allowed.

It is believed that no further additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they are authorized and may be charged to applicants' Deposit Account No. 07-0832.

Respectfully submitted,

By: /Guy H. Eriksen/
Guy H. Eriksen, Attorney for Applicants
Registration No.: 41,736
(609) 734-6807

Patent Operations
Thomson Licensing Inc.
P.O. Box 5312
Princeton, NJ 08543-5312

Date: March 20, 2009